

Assembly Bill No. 1950

CHAPTER 877

An act to add Section 1798.81.5 to the Civil Code, relating to privacy.

[Approved by Governor September 29, 2004. Filed
with Secretary of State September 29, 2004.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1950, Wiggins. Privacy: personal information.

Existing law regulates the handling of customer records and requires that a business take all reasonable steps to destroy a customer's records in its custody or control when they are no longer to be retained. Existing law requires a person or business that owns or licenses computerized data that include personal information, as defined, to disclose any breach of the security of its system, as specified.

This bill would require a business, other than specified entities, that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure. The bill would also require a business that discloses personal information to a nonaffiliated third party, to require by contract that those entities maintain reasonable security procedures, as specified. The bill would provide that a business that is subject to other laws providing greater protection to personal information in regard to subjects regulated by the bill shall be deemed in compliance with the bill's requirements, as specified.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.81.5 is added to the Civil Code, to read:

1798.81.5. (a) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information. For the purpose of this section, the phrase "owns or licenses" is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates.

(b) A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security



procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(d) For purposes of this section:

(1) “Personal information” means an individual’s first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(A) Social security number.

(B) Driver’s license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

(D) Medical information.

(2) “Medical information” means any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional.

(3) “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(e) The provisions of this section do not apply to any of the following:

(1) A provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).

(2) A financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code.

(3) A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

(4) An entity that obtains information under an agreement pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code and is subject to the confidentiality requirements of the Vehicle Code.



(5) A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with that state or federal law shall be deemed compliance with this section with regard to those subjects. This paragraph does not relieve a business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

